Editors: Matt Bishop, bishop@cs.ucdavis.edu
Deborah A. Frincke, deborah.frincke@pnl.gov

Combating the Insider Cyber Threat

FRANK L. GREITZER
Pacific Northwest National Laboratory

ANDREW P. MOORE AND DAWN M. CAPPELLI
Software Engineering Institute

DEE H. ANDREWS
Air Force Research Laboratory

LYNN A. CARROLL
Karta Technologies

THOMAS D. HULL
Oak Ridge Institute for Science and Education

The penetration of US national security by foreign agents as well as American citizens is a historical and current reality that's a persistent and increasing phenomenon. Surveys, such as the *E-Crime Watch Survey* (www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf), reveal that current or former employees and contractors are the second greatest cybersecurity threat, exceeded only by hackers, and that the number of security incidents has increased geometrically in recent years. The insider threat is manifested when human behavior departs from compliance with established policies, regardless of whether it results from malice or a disregard for security policies. The types of crimes and abuse associated with insider threats are significant; the most serious include espionage, sabotage, terrorism, embezzlement, extortion, bribery, and corruption. Malicious activities include an even broader range of exploits, such as copyright violations, negligent use of classified data, fraud, unauthorized access to sensitive information, and illicit communications with unauthorized recipients.

The "insider" is an individual currently or at one time authorized to access an organization's information system, data, or network; such authorization implies a degree of trust in the individual. The *insider threat* refers to harmful acts that trusted insiders might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual. A 1997 US Department of Defense (DoD) Inspector General report[1] found that 87 percent of identified intruders into DoD information systems were either employees or others internal to the organization. More generally, recent studies of cybercrime (such as the 2004 through 2006 *E-Crime Watch Surveys*; www.cert.org/archive/) in both government and commercial sectors reveal that although the proportion of insider events is declining (31 percent in 2004 and 27 percent in 2006), the financial impact and operating losses due to insider intrusions are increasing. Of those companies experiencing security events, the majority (55 percent) report at least one insider event (up from 39 percent in 2005).

In this article, we'll focus on the need for effective training to raise staff awareness about insider threats and the need for organizations to adopt a more effective approach to identifying potential risks and then taking proactive steps to mitigate them.

Training research

To help staff, management, and human resource personnel understand the social-behavioral factors and technical issues underlying insider threats, training on insider threat awareness and mitigation must be flexible and customizable to different roles and responsibilities. It should also be highly relevant and realistic and address privacy and legal issues. The question of how to effectively convey such complex knowledge and skills is tied to fundamental instructional systems design (ISD) issues with philosophical and theoretical roots to theorists such as Jean Piaget, John Dewey, and Lev Vygotsky,[2] who argued that learning contexts should be coupled with multiple opportunities for the learner to "construct" or discover meaning in the material (a constructivist or student-centered instructional philosophy) in contrast with the behaviorist or instructor-centered approach associated with traditional expository instruction.

Ongoing research at each of our institutions attempts to raise the bar in both training and insider research and development.

Pacific Northwest National Laboratory

PNNL has focused on interactive training in a variety of domains and predictive modeling for insider threat detection. Specifically, its researchers have developed complex, cognitive-based instruction to produce workshops and hands-on training, interactive computer-based training systems, and serious gaming approaches, blended training techniques,[3,4] and research on the effectiveness of game-based training.[5] For cybersecurity, an R&D initiative at PNNL (the In-

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2008	**Final**	**01-01-2007 to 31-12-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Combating the Insider Cyber Threat	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER **62202F**

6. AUTHOR(S)	5d. PROJECT NUMBER
Frank Greitzer; Andrew Moore; Dawn Cappelli; Dee Andrews; Lynn Carroll	**1123**
	5e. TASK NUMBER **AM**
	5f. WORK UNIT NUMBER **1123AM02**

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Air Force Research Laboratory/RHA,Warfighter Readiness Research Division,6030 South Kent Street,Mesa,AZ,85212-6061	**AFRL; AFRL/RHA**

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
Air Force Research Laboratory/RHA, Warfighter Readiness Research Division, 6030 South Kent Street, Mesa, AZ, 85212-6061	**AFRL; AFRL/RHA**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) **AFRL-RH-AZ-JA-2008-0003**

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Additional author: Hull, Thomas D. Published in IEEE Security and Privacy, 6(1), 61-64, Jan/Feb 2008

14. ABSTRACT
This article focuses on the premise that organizations must implement effective training to raise staff awareness about insider threats and the need for organizations to adopt a more effective approach to identifying potential risks and then taking proactive steps to mitigate them.

15. SUBJECT TERMS
Merit interactive; Training; Insider attack; CERT; Threat mitigation; Education; Cyber threat; Insider threats;

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Public Release**	**4**	

formation and Infrastructure Integrity Initiative) is advancing research on predictive and adaptive systems, including a project devoted specifically to cyber and behavioral modeling approaches to mitigate or predict malicious insider exploits.[6]

The MERIT workshop is an initial step toward more effective training about insider threat risk awareness and mitigation.

Carnegie Mellon University/Software Engineering Institute CERT Program

CERT has examined more than 200 cases of insider cybercrimes across US critical infrastructure sectors, focusing on both technical and behavioral aspects.[7,8] Ongoing work at CERT attempts to find effective mechanisms for communicating the results of this research to practitioners in government and industry through integrative models of the problem,[9,10] case studies and assessment of best practices,[11] and interactive instructional cases and games in which players are challenged to identify insider threat risks and take steps to mitigate them.[12] (See www.cert.org/insider_threat/ for a fuller description of CERT's insider threat research.)

US Air Force Research Laboratory

The AFRL has conducted considerable research into different approaches to training cognitive skills, to define better methods for measuring job skills as well as evaluate training programs. Additionally, it recently conducted a workshop to examine ways to incorporate storytelling into instruction, the results of which could help those who want to instruct managers about insider threats via games.

Training solutions in the insider threat domain

Recently, the authors of this article came together to advance their collective approaches and ideas to suggest innovative training solutions for the insider threat problem; an initial outcome is the preparation of this article. As we noted earlier, there's currently a paucity of training on insider threat for individuals with different roles and responsibilities within organizations. Although this problem is increasingly acknowledged within government and industry, much remains to be done. At the very least, the field needs more workshops and training courses to raise the awareness of management and human resources personnel about behavioral indicators and how to decrease risk; policies must be established to provide guidance for staff and management alike; and effective training is needed.

Workshops

Past research on insider threats has shown that managing insider threat risks within an organization is an extremely complex task characterized by limited information, complex feedback relationships, conflicting goals, and uncertain causal relationships. To address this, CERT developed an insider threat education and awareness workshop called MERIT (Management and Education of the Risks of Insider Threat)[9] and the materials presented at the Computer Security Institute's conference in November 2006 (www.cert.org/archive/pdf/CSInotes.pdf) based on previous empirical research on insider threats conducted at CERT and elsewhere.

The MERIT workshop focuses on insider IT sabotage and has the following structure:

- overview of empirical research on insider threat;
- interactive discussion of the instructional case of insider IT sabotage;
- general observations from case data;
- system dynamics model (problem, prevention, and mitigation); and
- recommendations for countering threats.

Our case study research and system dynamics modeling approach have helped to broaden our understanding of the insider threat problem and possible leverage points for its mitigation. We therefore characterize our offering as a workshop, rather than training, to emphasize that it focuses on interactive education and raising awareness of how organizations can mitigate the problem.

Games

The MERIT workshop is an initial step toward more effective training about insider threat risk awareness and mitigation. As Figure 1 shows, CERT also aims to bring the benefits of serious game technology to bear on the challenge of insider threat education. In collaboration with Carnegie Mellon's Entertainment Technology Center, CERT built a proof-of-concept game, called MERIT Interactive, that immerses players in a realistic business setting from which they make decisions about how to prevent, detect, and respond to insider actions and see how their decisions impact key performance metrics. It provides a team-oriented, role-playing experience using model-based

simulation of critical aspects of insider threat risk management in a realistic organizational context. Team orientation is critical because organizations typically identify these problems at an organizational enterprise level rather than an individual manager or department level. Role playing is also crucial because solutions generally require collaboration among multiple stakeholders; role playing helps players understand and acquire the necessary skills.

CERT is currently modifying the MERIT system dynamics model to serve as a back-end engine for MERIT Interactive. This should help transfer any insights the model provides into MERIT Interactive's learning objectives. Then, experiments will be carried out to assess the extent to which players have learned important lessons about the insider threat domain. We believe MERIT Interactive will ultimately help decision-makers better understand the effects their decisions have on risk—both its promotion and mitigation.

Clearly, a critical need exists for more effective organizational strategies to combat and prevent insider abuses. A complete and effective insider threat mitigation strategy must take into account human motivations and behaviors along with organizational factors such as policies, hiring, and training practices, and the technical vulnerabilities and best practices for prevention or early detection of unauthorized insider activity. We must conduct program evaluations to verify that we're teaching the right lessons, that staff behavior and attitudes reflect those training objectives, and that organizations ultimately benefit from these organizational strategies.

We must also recognize potential consequences and ethical issues surrounding possible mitigation strategies that could constrain users or systems or negatively impact productivity—for example, organizational responses to insider threat that might affect employee morale, or legal and privacy considerations associated with planned policies and IT measures. Ultimately, an organization must find solutions that provide a proper balance among the three system components of its response to insider threats (IT tools for predictive defense, organizational policies and practices, and management/staff training). □

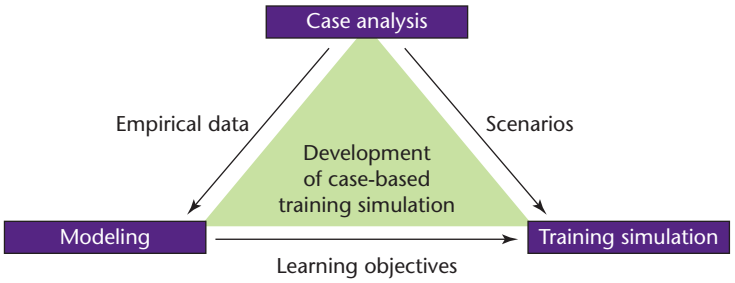

Figure 1. The MERIT Interactive approach provides a team-oriented, role-playing experience using model-based simulation of critical aspects of insider threat risk management. Informed by actual case studies, the simulated scenarios challenge players to understand and solve relevant problems in a realistic organizational context.

References

1. DoD Office of the Inspector General, *DoD Management of Information Assurance Efforts to Protect Automated Information Systems*, tech. report no. PO 97-049, US Dept. of Defense, Sept. 1997.
2. P.E. Doolittle and W.G. Camp, "Constructivism: The Career and Technical Education Perspective," *J. Vocational and Technical Education*, vol. 16, no. 1, 1999; http://scholar.lib.vt.edu/ejournals/JVTE/v16n1/doolittle.html.
3. F.L. Greitzer, D.J. Pond, and M. Jannotta, "Scenario-Based Training on Human Errors Contributing to Security Incidents," *Proc. Interservice/Industry Training, Simulation, and Education Conf.* (I/ITSEC 04), 2004; http://ntsa.metapress.com/app/home/contribution.asp?referrer=parent&backto=issue,130,174;journal,4,8;linkingpublicationresults,1:113340,1.
4. F.L. Greitzer et al., "Learning to Pull the Thread: Application of Guided-Discovery Principles to the Inquiry Process," *Proc. Interservice/Industry Training, Simulation, and Education Conf.* (I/ITSEC 05), 2005; www.simsysinc.com/IITSEC/ED2005.htm#_Toc118714554.
5. F.L. Greitzer, O.A. Kuchar, and K. Huston, "Cognitive Science Implications for Enhancing Training Effectiveness in a Serious Gaming Context," *ACM J. Educational Resources in Computing*, vol. 7, no. 3, Article 2, August 2007; http://portal.acm.org/citation.cfm?id=1281320.1281322&coll=&dl=ACM&idx=J814&part=journal&WantType=Journals&title=Journal%20on%20Educational%20Resources%20in%20Computing%20(JERIC).
6. F.L. Greitzer et al., *Predictive Adaptive Classification Model for Analysis and Notification: Internal Threat*, tech. report PNNL-16713, Pacific Northwest National Lab., 2007.
7. M. Keeney et al., *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, tech. report, U.S. Secret Service and Carnegie Mellon Univ., Software Eng. Inst., 2005; www.secretservice.gov/ntac/its_report_050516.pdf.
8. M.R. Randazzo et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, tech. report no. CME/SEI-2004-TR-021,

Carnegie Mellon Univ., Software Eng. Inst., 2004; www.sei.cmu.edu/publications/documents/04.reports/04tr021.html.
9. A.P. Moore et al., "An Experience Using System Dynamics Modeling to Facilitate an Insider Threat Workshop," *Proc. 25th Conf. System Dynamics Soc.*, The System Dynamics Society, 2007; www.cert.org/archive/pdf/ISDC2007.pdf.
10. S.R. Band et al., *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis*, tech. report CMU/SEI-2006-TR-026, Carnegie-Mellon Univ., Software Eng. Inst., 2006.
11. D.M. Cappelli, A.P. Moore, and T.J. Shimeall, *Common Sense Guide to Prevention/Detection of Insider Threats*, tech. report, Carnegie Mellon Univ., CyLab and the Internet Security Alliance, July 2006; www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf.
12. D. Cappelli et al., "Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage," *Proc. 24th Conf. System Dynamics Soc.*, The System Dynamics Society, 2006; www.cert.org/archive/pdf/merit.pdf.

Frank L. Greitzer *is a chief scientist at the Pacific Northwest National Laboratory (PNNL). His research interests include human behavior modeling, system evaluation methods and metrics, and modeling human cyber behavior with application to identifying malicious insider activities. Greitzer has a a BS in mathematics from Harvey Mudd College and a PhD in mathematical psychology with specialization in memory and cognition from the University of California, Los Angeles. He is an editorial board member of the* Journal of Cognitive Informatics & Natural Intelligence. *Contact him at frank.greitzer@pnl.gov.*

Andrew P. Moore *is a senior member of the technical staff of CERT at the Software Engineering Institute at Carnegie Mellon University. His interests include improving security, survivability, and resiliency of enterprise systems through attack and defense modeling, and incident processing and analysis. Moore has a BA in mathematics from the College of Wooster and an MA in computer science from Duke University. Contact him at apm@cert.org.*

Dawn M. Cappelli *is senior member of the technical staff in CERT at Carnegie Mellon University's Software Engineering Institute (SEI). She is technical lead of CERT's insider threat research and is also adjunct professor in Carnegie Mellon's Heinz School of Public Policy and Management. Cappelli has a BS in mathematics and computer science from the University of Pittsburgh. Contact her at dmc@sei.cmu.edu.*

Dee H. Andrews *is senior scientist at the Human Effectiveness Directorate at the Air Force Research Laboratory in Mesa, Arizona. His research interests include training in distributed environments, instructor-operator station design, performance measurement, command and control, cost effectiveness, and decay and retention of higher order cognitive skills. Andrews has a PhD in instructional systems from Florida State University. Contact him at dee.andrews@mesa.afmc.af.mil.*

Lynn A. Carroll *is a consultant with Karta Technologies. Previously, he was a fighter pilot the US Air Force, and served in Thailand and the Republic of Korea where he commanded the 604th Direct Air Support Squadron and served at the Pentagon, where he oversaw Air Force simulation and training programs. He is the author of* Entertaining War: Let the Games Begin. *Contact him at lynnalncrl@aol.com.*

Thomas D. Hull *is a graduate fellow with the Oak Ridge Institute for Science and Education and works jointly with the Human Effectiveness Directorate at the Air Force Research Laboratory in Mesa, Arizona. His research focuses on the use of storytelling as instruction in computer simulation and problem-based learning environments, training management for insider threat and cybersecurity risks within a dynamic models framework, and current trends in instructional system design models. Hull has a BA in anthropology from Northern Arizona University. Contact him at thomas.hull@mesa.afmc.af.mil.*